1

HP Encryption
Smart Card Security System

User’s Guide

Before You Begin

Package Contents

Your Encryption Smart Card Security System package contains:

- 1 PCMCIA smart card reader
- 2 GPK4000 smart cards (one spare card for backup/recovery purposes)
- 1 CD-ROM containing the Encryption Smart Card Security System software
- 1 User's Guide (this manual)

An optional pack of five smart cards is also available as a separate OmniBook accessory (order no. F1613A).

System Requirements

To install the Smart Card Security System, you need:

- An OmniBook 900 or 4150 or later with Windows 95 OSR2, Windows 98, or Windows NT 4.0 (a Smart Card BIOS is included), or

  An OmniBook 2100, 3100, 4100, 7100, 7150 with Windows 95 OSR2, Windows 98, or Windows NT 4.0 (BIOS security features require a Smart Card BIOS, not included), or

  An OmniBook XE with Windows 98. BIOS security features are not supported. Future models may support other operating systems and BIOS security.
- A CD-ROM drive installed in your OmniBook or available via a network (on certain OmniBook models the CD-ROM drive is an option that must be purchased separately).
- 1 free PCMCIA slot
- At least 7 megabytes of free hard disk space

HP also recommends that you have a formatted floppy diskette on hand to use as a safe place to store the recovery file generated during the smart card setup process.

The HP Encryption Smart Card Security System

With the HP Encryption Smart Card Security System, your smart card can provide several types of security for your OmniBook. The security you have available depends on your operating system, your security setup options, and your system BIOS.

- **BIOS Security**

  These features require a Smart Card BIOS, which is not available for all OmniBook models. If you don't have a Smart Card BIOS, you can use the normal BIOS password for BIOS security.

  Startup authorization.
  Resume authorization.
  Undock authorization.
  BIOS Setup authorization.

- **Windows NT Security**

  Logon authorization.
  Secure screen saver.
  Lock at card removal.

- **Windows 95/98 Security**

  Secure screen saver.
  Lock at card removal.

- **Encryption Security**

  Data encryption.
  Lock at card removal.

Overview of the Setup Procedure

Windows NT requires that an NT administrator set up the Smart Card Security System on an OmniBook. For a Windows 95/98 system, setup can be performed by the user.

To ensure the setup procedure is successful, the following steps must be completed in order:

1. Install the drivers, software, and PCMCIA card reader
2. Initialize a smart card (Windows NT)
3. Update your OmniBook's system BIOS
4. Enable BIOS smart card security
5. Set up a Secure folder on your hard disk
6. Make a recovery file

These steps are discussed on the following pages.

Caution **Do not insert your smart card reader until instructed to do so by the installation program.**

Step 1: Install the drivers, software, and PCMCIA card reader

Caution **Do not insert your smart card reader until instructed to do so by the installation program.**

1. Start your OmniBook (for Windows NT, log on as Administrator) and wait for your Windows desktop to display.
2. Insert the Smart Card Security System CD. If your CD-ROM drive is configured to "autorun", the smart card installation process will begin automatically. If it is not, use Windows Explorer to browse the CD contents and double-click the file *setup.exe* in the root directory to run the installation.
3. Click "Install HP Encryption Smart Card Security System" to start the setup.
4. When the installation process asks you to install the PCMCIA card reader, make sure the label is facing up.

For Windows NT, if Service Pack 4 (SP4) is not installed, the system will prompt you to let it be installed from the Smart Card Security System CD.

Your Secure folder will be C:\Private by default, but may be changed during installation if desired.

Your OmniBook will be restarted when the installation is complete.

Step 2: Initialize a smart card (Windows NT)

For Windows 95/98, go to "Step 3" on page 8.

A smart card can be initialized only after the software has been installed and your OmniBook has been restarted (Step 1).

1. For Windows NT, if you have just installed the software and your OmniBook has been restarted, you will be asked to insert an uninitialized smart card into the card reader. Insert the card face-up and so the end nearest the gold memory emblem goes in first.
2. Enter the card holder's name and a PIN (personal identification number). The name is permanent and can not be changed. The PIN must be exactly eight digits long and contain only numbers. You must enter the PIN twice for verification.
3. Click **OK**.

Note Memorize your PIN! You will not be able to use your smart card to gain access to your OmniBook if you forget the PIN. You may wish to write the PIN on a piece of paper and keep it in a safe place, such as a safety deposit box.

4. Enter the NT logon name, password, and domain name, followed by the card's PIN.
5. Click **OK**.

The smart card is now ready for use.

Initializing Further Smart Cards

You can initialize as many cards as you want. Each authorized user can have their own smart card with user name and PIN. Two blank uninitialized smart cards are provided with the Smart Card Security System.

Once you have initialized the first smart card, you can initialize further cards at any time as follows:

1. Log on to your OmniBook using your smart card.
2. Click Start, Programs, HP Security System, Smart Card Security Manager to run the Smart Card Security Manager.
3. For Windows NT, click the **NT Logon** tab, then click **Options**. Change the "On card removal" setting to "Continue."

   For Windows 95/98, click the **Win95/98** tab. Disable the option "Launch screen saver on smart card removal."
4. Insert an uninitialized smart card into the reader.
5. Click the **Smart Card** tab.
6. Click **Initialize**.
7. Follow the instructions to initialize the card.
8. On the **NT Logon** or **Win 95/98** tab, restore the card-removal setting you changed above.

Multiple Accounts on a Single Smart Card

You can create multiple NT logon accounts on a single card. Each account has its own user name, password and domain. This means you can access several different accounts with one smart card.

For further information, refer to the online help.

Step 3: Update your OmniBook's system BIOS

For an OmniBook 900 or 4150 with a BIOS version earlier than 2.20, or for an OmniBook with a Smart Card BIOS available on the OmniBook website, www.hp.com/omnibook, update the BIOS to support BIOS security features. To determine your BIOS version, reboot the computer and press F2 when you see the HP logo—the first screen of BIOS Setup shows the BIOS version.

Skip these steps if your BIOS is a Smart Card BIOS or if none is available for your model.

Follow these steps to update your BIOS:

1. Start Windows Explorer.
2. Insert the Smart Card Security System CD and run *setup.exe*.
3. In the Smart Card Setup window, click the "Smart Card BIOS Update" option.

Caution **Your OmniBook must be on ac power during BIOS update because a power loss will completely disable your OmniBook computer.**

4. Follow the displayed instructions to create a BIOS update floppy and update the BIOS.

Step 4: Enable BIOS smart card security

This step must be performed by the BIOS administrator. Follow these steps to enable BIOS smart card security on your OmniBook (if it is supported):

1. Click Start, Programs, HP Security System, Smart Card Security Manager to run the Smart Card Security Manager.
2. Click the **BIOS Password** tab.
3. Insert a smart card into the reader. Ensure this card is the one you want to be the BIOS Administrator card. For Windows NT, this could be the NT administrator card.
4. If the **Enable** button is dimmed, BIOS security is not supported. Skip to "Step 5" on page 10.
5. Click **Enable** to create the BIOS Administrator card.

Note For ease of use, HP recommends that you do *not* enable the option requiring the PIN at boot. The presence of the card unlocks the computer.

Setting Up a BIOS User Password Card

Follow these steps to set up a BIOS user password in the BIOS and store it on a smart card.

1. Click Start, Programs, HP Security System, Smart Card Security Manager to run the Smart Card Security Manager.
2. Click the **BIOS Password** tab.
3. Click **Set** next to "BIOS User Password" and follow the instructions to create a BIOS user password card. You must have the BIOS administrator card available.

Step 5: Set up a Secure folder on your hard disk

The Secure folder holds files that are automatically encrypted. The encryption key is kept on the user smart card.

1. Insert your user smart card into the reader.
2. Click Start, Programs, HP Security System, Smart Card Security Manager to run the Smart Card Security Manager.
3. Click the **Encryption** tab.
4. Click **Create** and follow the instructions.

Step 6: Make a recovery file

Note HP strongly recommends you make a new encrypted recovery file of your smart card data now and also whenever you change a smart card password. This recovery file will allow you to recreate your smart card (and, more importantly, access your computer) if the card is lost, stolen, or damaged. You can keep old recovery files in case you need to create an old card.

Even if you created a recovery file earlier, you should make another one now to ensure it includes all the latest information entered up to this point.

To make a recovery file of your smart card:

1. Click Start, Programs, HP Security System, Smart Card Security Manager to run the Smart Card Security Manager.
2. Click the **Smart Card** tab.
3. Insert a formatted floppy disk in the floppy drive.
4. In the **Recovery** section, click **Create** and follow the instructions. The recovery file is encrypted and saved on the floppy disk.
5. Store the floppy disk in a safe place.

Note Memorize the recovery file password! You will not be able recreate your smart card from the recovery file if you forget the password. You may wish to make a note of the password on a piece of paper and keep it in a safe place, such as a safety deposit box.

Do not save the recovery file on your OmniBook's hard disk because you will not be able to access the file without your smart card. Furthermore, the recovery file may be accessible to others, which can pose a security risk.

Using Your Smart Card

When properly set up, the HP Smart Card Security System ensures only users with your smart card and the correct PIN (personal identification number) can use your OmniBook. See page 15 for setup options.

Starting or Logging On To Your OmniBook

To start or log on to your OmniBook, insert your smart card into the reader and enter your PIN if prompted.

Note If the PIN is entered incorrectly seven times, the smart card will be automatically locked (disabled) to ensure the OmniBook's security. Once disabled, the smart card is *permanently unusable* and should be discarded.

If you don't have a smart card BIOS, the normal BIOS password and NT logon provide security.

Logging Off or Locking Your OmniBook

To lock your OmniBook, remove your card from the reader. The OmniBook will automatically lock—if the Smart Card Security Manager is configured to do this. Or you can allow the secure screen saver to activate.

For Windows NT users, the NT logon options can be changed only by the administrator.

Undocking Your OmniBook or Resuming From Suspend

To undock your OmniBook or resume from suspend, you must insert the smart card into the reader and enter your PIN.

Note that you cannot undock your OmniBook while in MS-DOS mode. First exit back to Windows, then undock.

Note Do not leave the OmniBook unattended in MS-DOS mode. The Smart Card Security System is inactive in this mode.

If you don't have a Smart Card BIOS, the normal BIOS password provides security.

Using the Secure Folder

By default, your Secure folder is located in C:\Private.

After you have inserted your smart card and correctly entered your PIN, you can create directories and files within the Secure folder in exactly the same way as outside the Secure folder. The following guidelines apply.

Storing existing files in the Secure folder

Use your application or Windows Explorer to **Save as** or **Copy to** the Secure folder. Windows NT will also allow you to move files using drag and drop.

Note that **Save as** can and **Copy to** will leave a copy of your document in the unsecure part of your hard disk, which presents a potential security risk.

If you move files out of your Secure folder they are decrypted.

Using an existing file in the Secure folder

Use your application to **Open** and then **Save** or **Save as** files stored in your Secure folder just like you would files in any other folder. Files are encrypted when they're saved.

Deleting a file in the Secure folder

Use **Shift**+**Delete** to permanently delete files from your Secure folder and not send them to the Recycle Bin.

Note Do not use **Delete** to remove files from your Secure folder because this would decrypt the files and place them in the Recycle Bin.

Backing up secure files

It is a good idea to back up files in your Secure folder just like you do all your other files. However, you should back up your Secure folder and all its contents separate from your unsecure files, then keep the decrypted backup files in a secure place. Make sure your smart card is inserted during the backup to ensure files are decrypted properly.

Using the Smart Card Security Manager

Note HP recommends that you *not* change the default administrator settings in the Smart Card Security Manager unless you are familiar with NT logon practices.

At the desktop, access the Smart Card Security Manager by clicking Start, Programs, HP Security System, Smart Card Security Manager.

Smart Card Options

To see the following options, click the **Smart Card** tab in the Smart Card Security Manager.

Initialize a Smart Card

A smart card must be initialized before it can be used. This option is activated only if the administrator settings in the Smart Card Security Manager allow it. Refer to page 6 for instructions.

Change a Smart Card's PIN

You can change your smart card's PIN (Personal Identification Number). The PIN must be exactly eight digits long and can contain only numbers. To change the PIN:

1. Run the Smart Card Security Manager and click the **Smart Card** tab.
2. Click **Change PIN**.
3. Enter the old PIN, then the desired PIN (twice).
4. Click **OK**.

Create a Recovery File

It is strongly recommended that you create a recovery file after creating a new smart card or changing a smart card's data. The recovery file will allow you to recreate your smart card if it is lost or stolen. Refer to page 11 for instructions.

Restore a Smart Card

You can create a duplicate smart card from a recovery file. This is especially useful if your card was lost or stolen, or if you simply want to create a backup smart card, ready for use.

Before starting, you will need:

- Access to a computer that has the Smart Card Security System reader and software installed.
- The floppy disk containing the recovery file.
- An uninitialized OmniBook smart card. You can't use a disabled card.

Note If you use a smart card that is not blank, the original contents of the card (such as logon name, password, and encryption key) will be deleted during the recovery process. The card's user name and PIN will not change.

To restore a smart card:

1. Click Start, Programs, HP Security System, Smart Card Security Manager to run the Smart Card Security Manager.
2. For Windows NT, click the **NT Logon** tab, then click **Options**. Change the "On card removal" setting to "Continue."

   For Windows 95/98, click the **Win95/98** tab. Disable the option "Launch screen saver on smart card removal."
3. Click the **Smart Card** tab.
4. Insert the floppy disk containing the recovery file in the floppy drive.
5. Insert the smart card into the reader.
6. In the **Recovery** section, click **Restore**.

7. Ensure the correct recovery file name is selected.
8. Enter the recovery file's password (the one you entered when you created the recovery file) and click **OK**.
9. On the **NT Logon** or **Win 95/98** tab, restore the card-removal setting you changed above.

The original smart card contents will be restored to the new smart card.

BIOS Password Options

To see these options, click the **BIOS Password** tab in the Smart Card Security Manager.

These options allow you to do the following:

- Enable or disable BIOS smart card security. This is a BIOS administrator option. Note that disabling this option clears all BIOS passwords.
- Change the BIOS administrator or user password stored in the BIOS.
- Store or change a BIOS password on a smart card. Note that changing your card's password will make it unable to unlock your computer.
- Change whether the smart card's PIN must be entered to boot the OmniBook. For ease of use, leave this option disabled. The PIN is still required to start Windows NT.

See the online help for more information.

NT Logon Options

To see these options, click on the **NT Logon** tab in the Smart Card Security Manager. This tab appears only for Windows NT.

These options allow you to add and remove Windows NT accounts from your smart card. This means you can use your smart card to log on to several different Windows NT accounts, as well as change the password for any of these accounts.

All other NT Logon options are disabled for the user and can be changed only by the administrator.

Win 95/98 Options

To see these options, click the **Win 95/98** tab in the Smart Card Security Manager. This tab appears only for Windows 95 or 98.

These options allow you to do the following:

- Enable or disable the secure screen saver. The secure screen saver provides smart card security whenever you remove the card and when the screen saver activates.
- Enable or disable smart card security when undocking or when resuming operation after the computer suspends.

See the online help for more information.

Encryption Options

To see these options, click the **Encryption** tab in the Smart Card Security Manager.

These options allow you to do the following:

- Create a new encryption key. The new key cannot decrypt files created with a different key.
- Specify when the Secure folder locks. You can make the Secure folder lock as soon as the card is removed, or it can remain unlocked until logoff.

See the online help for more information.

Documentation and Help

There are several sources of documentation and help for the HP Smart Card Security System:

- The online help contains information about using and configuring the Smart Card Security System.

  The online help is installed on your OmniBook when you install the Smart Card Security System.

  You can also access the online help in the **\DOC** directory on the Smart Card Security System CD.

- HP's web site resources, including software and drivers, manuals, FAQs (Frequently Asked Questions) and technical notes. There is also information about HP's *Smart Card Ready* program. Go to http://www.hp.com/omnibook/security.

Troubleshooting

If you are experiencing any problems with your OmniBook, *do not* log off or remove your smart card until the problem has been resolved.

Additional troubleshooting information is available in the online help.

Problem	Explanation	Action
I lost my smart card.	If you are using NT, you will now be unable to log on to your NT account and gain access to your OmniBook. You will also be unable to read the files in your Secure folder.	Make a new card on another OmniBook with a Smart Card Security System using your recovery file (see page 16). If you can't do this, contact your system administrator to regain access using the administrator card. If the computer will not unlock, call HP for assistance in restoring the BIOS password. Then make a new card using the recovery file. If no recovery file is available, encrypted data is not recoverable.
	If you are using Windows 95/98, you will be unable to read the files in your Secure folder and may not be able to start the computer.	Make a new card on another OmniBook with a Smart Card Security System using your recovery file (see page 16). If the computer will not unlock, use an administrator card or call HP for assistance in restoring the BIOS password. Then make a new card using the recovery file. If no recovery file is available, encrypted data is not recoverable.
I cannot log on to my NT account.	You are not using the correct card, your smart card is not inserted correctly in the smart card reader, or the reader is not connected correctly to the OmniBook.	Check your smart card. Check that the card is correctly inserted in the reader and the reader is correctly inserted in the PCMCIA slot.

Problem	Explanation	Action
I could not remember my PIN, I tried to enter it seven times and now my card no longer works.	As a security measure to prevent someone who has obtained your smart card from guessing your PIN, you are allowed only seven attempts at entering the correct PIN. If you fail to enter the correct PIN on the seventh attempt, your card is locked.	Use the recovery file to create a new card.
Access to your Secure folder is denied.	The Smart Card Security Manager is unable to retrieve information stored on the smart card.	Make sure your smart card is properly inserted in the reader and the correct PIN has been entered. If this isn't done, you will not be able to access the Secure folder. If you are still unable to access the Secure folder, you may have corrupted information on your smart card. Use the recovery procedure detailed on page 16 to restore your smart card.
Files copied into the Secure folder don't seem to be encrypted.	The smart card you used to move your files into the Secure folder is still inserted in the reader, and you still have access to all the files you moved into the Secure folder.	Insert a card with a different encryption key into the reader and check the content of your files: they should be unreadable.
Encrypted text decrypts badly.	The card inserted in the reader is not the one you used to encrypt your files.	Insert the correct card and enter your PIN to access the Secure folder.
I can't delete a file in my Secure folder using the Delete key.	For security reasons, deleting files using Delete is not recommended (it would leave a copy in the Recycle Bin).	To delete a file from the Secure folder use Shift+Delete.
A message tells me that access to the smart card is denied.	The Smart Card Security Manager is unable to retrieve information stored on the smart card.	Check that the smart card is correctly inserted in the reader and the reader is correctly inserted in the PCMCIA slot. Insert the card face-up and so the end nearest the gold memory emblem goes in first.

Problem	Explanation	Action
Nothing happens when I insert my smart card.	Your smart card is incorrectly inserted in the reader.	Ensure you have inserted the smart card correctly. Try removing and reinserting it, face-up and so the end nearest the gold memory emblem goes in first.
	The smart card reader is incorrectly installed in the PCMCIA slot.	Ensure the reader is correctly connected and fully inserted in your OmniBook's PCMCIA slot.
At startup, no smart card is detected.	The smart card, card reader, or PCMCIA slot is bad, or there is a conflict with another device.	Reinsert the card, face-up and so the end nearest the gold memory emblem goes in first. Reinsert the card reader in the slot. Make sure it is fully inserted. Check device configurations in Windows. The reader must use I/O address 0300. Change the address of a LAN card or other device that uses address 0300. If another system is available, open Smart Card Security Manager and insert your reader and card. Check whether they are detected properly. Call HP for repair assistance.
My PIN is not accepted.	You are using the wrong smart card.	Check the user name displayed at the PIN prompt.
I can't open Smart Card Security Manager to disable BIOS security.	The hard disk has a problem.	Insert the BIOS administrator card. Reboot the computer and press F2 to run BIOS setup, then disable BIOS security.

Getting HP OmniBook Assistance

Support Assistance

If you need assistance with your HP OmniBook or accessory, use any of the following support services:

	Provider Type	Type of Assistance
1.	"Electronic Support Services" described below	HP self-help tools, information and software Approved and Tested Solutions
2.	"Customer Support Services" described below	Telephone support assistance In and out of warranty repair processes
3.	HP-authorized resellers	Local support assistance Referral to Customer Support Center or HP-approved support provider

Electronic Support Services

HP OmniBook World Wide Web: Download technical information, drivers and software from the web at www.hp.com/omnibook.

HP OmniBook & Peripheral Self-Help and Direct-Help Tools: Visit the web at: http://www.hp.com/cpso-support/guide/home.html.

- **Choose Self-Help Tools** to use a number of services that offer information and software that will help you make the most of your HP products.
  - The HP FIRST Fax Retrieval System - (800) 333-1917 (inside U.S. and Canada) - (208) 344-4809 (outside U.S. and Canada)
  - Bulletin Boards
  - Commercial Online Services

- CD-ROM Subscriptions
- Service Parts Information

- **Choose Talk to HP Directly** for information about how to contact HP for telephone assistance from our technical Customer Support Centers, or for receiving drivers and software by mail.
  - Customer Support Centers
  - Software Distribution

Customer Support Centers

HP Customer Support Centers, will assist you for free (you are responsible for the telephone charges) during the term of the warranty. Refer also to http://www.hp.com/cpso-support/guide/home.html.

During the free assistance period, HP will assist with questions about:	HP will not be able to help with questions about:
Included applications and operating systems.	Non-HP hardware, software, operating systems, or usage not intended for or included (by HP) with the product.
HP-described operation environments and conditions.	How to repair the product yourself.
HP accessories, HP upgrades, and basic operation and troubleshooting.	Product development, custom installations.
	Consulting.

US/Canada	
English	(970) 635-1000
French (Canada)	(800) 387-3867
Asia-Pacific	+1 (970) 635-1000
Europe	
Belgium (Dutch)	02 626 8806
Belgium (French)	02 626 8807
Denmark	3929 4099
Finland	0203 47 288
France	01 43 62 34 34
Germany	0180 52 58 143
Italy	02 264 10350
Norway	22 11 6299
Spain	902 321 123
Sweden	08 619 2170
United Kingdom	0171 512 52 02
Latin America	+1 (970) 635-1000
Other countries	+1 (970) 635-1000

Repair Assistance

Warranty. You must contact one of the participating support providers listed in item 2 in "Support Assistance" on page 23, or an HP Service Center to receive warranty service. The support provider will help qualify your unit for warranty repair based on the warranty applicable to your unit and original purchase date, and will provide you with repair processes in your area. Warranty service includes the cost of shipping, handling, duties, taxes, freight and/or fees to or from the service location.

Out of Warranty. Contact one of the support providers listed in items 2 or 3 in "Support Assistance" on page 23, or an HP Service Center. The support provider will provide you with repair charges and processes in your area.

HP Limited Warranty Statement

1. HP warrants to you, the end-user customer, that HP hardware, accessories and supplies will be free from defects in materials and workmanship after the date of purchase, for the period specified in the Warranty Duration sheet included with your OmniBook. If HP receives notice of such defects during the warranty period, HP will, at its option, either repair or replace products which prove to be defective. Replacement products may be either new or equivalent in performance to new.
2. HP warrants to you that HP software will not fail to execute its programming instructions after the date of purchase, for the period specified in the Warranty Duration sheet included with your OmniBook, due to defects in material and workmanship when properly installed and used. If HP receives notice of such defects during the warranty period, HP will replace software which does not execute its programming instructions due to such defects.
3. HP does not warrant that the operation of HP products will be uninterrupted or error free. If HP is unable, within a reasonable time, to repair or replace any product to a condition as warranted, you will be entitled to a refund of the purchase price upon prompt return of the product.
4. HP products may contain remanufactured parts equivalent to new in performance or may have been subject to incidental use.
5. Warranty does not apply to defects resulting from (a) improper or inadequate maintenance or calibration, (b) software, interfacing, parts or supplies not supplied by HP, (c) unauthorized modification or misuse, (d) operation outside of the published environmental specifications for the product, or (e) improper site preparation or maintenance.
6. TO THE EXTENT ALLOWED BY LOCAL LAW, THE ABOVE WARRANTIES ARE EXCLUSIVE AND NO OTHER WARRANTY OR CONDITION, WHETHER WRITTEN OR ORAL, IS EXPRESSED OR IMPLIED AND HP SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, AND FITNESS FOR A PARTICULAR PURPOSE. Some countries, states or provinces do not allow limitations on the duration of an implied warranty, so the above limitation or exclusion might not apply to you. This warranty gives you specific legal rights and you might also have other rights that vary from country to country, state to state, or province to province.
7. TO THE EXTENT ALLOWED BY LOCAL LAW, THE REMEDIES IN THIS WARRANTY STATEMENT ARE YOUR SOLE AND EXCLUSIVE REMEDIES. EXCEPT AS INDICATED ABOVE, IN NO EVENT WILL HP OR ITS SUPPLIERS BE LIABLE FOR LOSS OF DATA OR FOR DIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL (INCLUDING LOST PROFIT OR DATA), OR OTHER DAMAGE, WHETHER BASED IN CONTRACT, TORT, OR OTHERWISE. Some countries, states or provinces do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

   THE WARRANTY TERMS CONTAINED IN THIS STATEMENT, EXCEPT TO THE EXTENT LAWFULLY PERMITTED, DO NOT EXCLUDE, RESTRICT OR MODIFY AND ARE IN ADDITION TO THE MANDATORY STATUTORY RIGHTS APPLICABLE TO THE SALE OF THIS PRODUCT TO YOU.

In addition to the Limited Warranty Statement above, and to the extent permitted by local law, Hewlett-Packard Company expressly disclaims any warranty that this product will be error-free. Hewlett-Packard Company makes no warranty that any data stored or encrypted by this product will be recoverable or accessible, or that access provided by this product will be maintained.

The Gemplus smart card reader is not covered by the HP Limited Warranty Statement above. Refer to the Gemplus Limited Warranty Statement included with the reader.

HP Software License Agreement

CAREFULLY READ THIS LICENSE AGREEMENT BEFORE PROCEEDING TO OPERATE THE HP ACCESSORY. RIGHTS IN THE SOFTWARE ARE OFFERED ONLY ON THE CONDITION THAT THE CUSTOMER AGREES TO ALL TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. PROCEEDING TO INSTALLING AND USING THE ACCESSORY INDICATES YOUR ACCEPTANCE OF THESE TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO THE LICENSE AGREEMENT, YOU MUST NOW DESTROY ANY MASTER DISKETTES OR CD-ROMS, OR RETURN THE COMPLETE ACCESSORY AND SOFTWARE FOR A FULL REFUND.

UNLESS OTHERWISE STATED BELOW, THIS HP SOFTWARE PRODUCT LICENSE AGREEMENT SHALL GOVERN THE USE OF ALL SOFTWARE THAT IS PROVIDED TO YOU, THE CUSTOMER, AS PART OF THE HP ACCESSORY. IT SHALL SUPERSEDE ANY NON-HP SOFTWARE LICENSE TERMS THAT MAY BE FOUND ON-LINE, OR IN ANY DOCUMENTATION OR OTHER MATERIALS CONTAINED IN THE ACCESSORY PRODUCT PACKAGING.

Note: Any software provided by Microsoft is licensed to you under the Microsoft End User License Agreement (EULA) contained in the Microsoft documentation.

The following License Terms govern the use of the software:

USE. Customer may use the software on any one computer. Customer may not network the software or otherwise use it on more than one computer. Customer may not reverse assemble or decompile the software unless authorized by law.

COPIES AND ADAPTATIONS. Customer may make copies or adaptations of the software (a) for archival purposes or (b) when copying or adaptation is an essential step in the use of the software with a computer so long as the copies and adaptations are used in no other manner.

OWNERSHIP. Customer agrees that he/she does not have any title or ownership of the software, other than ownership of the physical media. Customer acknowledges and agrees that the software is copyrighted and protected under the copyright laws. Customer acknowledges and agrees that the software may have been developed by a third party software supplier named in the copyright notices included with the software, who shall be authorized to hold the Customer responsible for any copyright infringement or violation of this Agreement.

TRANSFER OF RIGHTS IN SOFTWARE. Customer may transfer rights in the software to a third party only as part of the transfer of all rights and only if Customer obtains the prior agreement of the third party to be bound by the terms of this License Agreement. Upon such a transfer, Customer agrees that his/her rights in the software are terminated and that he/she will either destroy his/her copies and adaptations or deliver them to the third party.

SUBLICENSING AND DISTRIBUTION. Customer may not lease, sublicense the software or distribute copies or adaptations of the software to anyone in physical media or by telecommunication without the prior written consent of Hewlett-Packard.

TERMINATION. Hewlett-Packard may terminate this software license for failure to comply with any of these terms provided Hewlett-Packard has requested Customer to cure the failure and Customer has failed to do so within thirty (30) days of such notice.

UPDATES AND UPGRADES. Customer agrees that the software does not include updates and upgrades which may be available from Hewlett-Packard under a separate support agreement.

EXPORT CLAUSE. Customer agrees not to export or re-export the software or any copy or adaptation in violation of the U.S. Export Administration regulations or other applicable regulation.

U.S. GOVERNMENT RESTRICTED RIGHTS. Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013. Hewlett-Packard Company. 3000 Hanover Street, Palo Alto, CA 94304 U.S.A. Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

(9 Nov 1998)

HP Software License Agreement